15

5

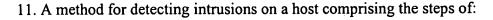
CLAIMS

- 1. A system for detecting intrusions, comprising:
 - a) a signature computing function configured to compute a file signature for a file;
 - b) a storage for storing a first file signature previously computed by the signature computing function for the file;
 - a storage for storing a second file signature previously computed by other than the signature computing function for the file; and
 - d) an analysis engine configured to compare the computed file signature to the first and second previously computed file signatures.
- 2. The system as recited in claim 1, wherein the storage for the second previously computed file signature is a package management database.
- 3. The system as recited in claim 2, wherein the package management database is at a remote location from the host.
- 4. The system as recited in claim 2, wherein the storage for the first previously computed file signature is an internal database.
- 5. The system as recited in claim 4, wherein the internal database includes signatures for files previously computed by other than the signature computing function.

15

- 6. The system as recited in claim 1, wherein the first file signature is previously computed from an archival file.
- 7. A system for detecting intrusions, comprising:
- a) a package management database including a previously computed signature for a file;
 - b) a database of exceptions; and
 - c) an analysis engine configured to compute a current signature for the file, compare the computed signature to the previously computed signature, and if there is a mismatch between the computed and previously computed signatures, check the mismatch against the database of exceptions.
 - 8. The system as recited in claim 7, wherein the database of exceptions includes a plurality of rules.
 - 9. The system as recited in claim 8, wherein the database of exceptions further includes a rule categorizing some types of files as expected to change, and other types of files as expected to remain constant.
- 20 10. The system as recited in claim 9, wherein the analysis engine is further configured to use information from a file type, filename, and file type categorization to compute a suspicion level associated with a change in the file.

5



- a) providing a signature computer;
- b) computing a signature of a file with the signature computer;
- c) comparing the computed signature to a file signature previously computed by the signature computer; and
- d) comparing the computed signature to a file signature previously computed by other than the signature computer.

12. A method for detecting intrusions, comprising the steps of:

- a) storing a previously computed signature for a file;
- b) providing a database of exceptions;
- c) computing a current signature for the file;
- d) comparing the computed signature to the previously computed signature; and
- e) if there is a mismatch between the computed and previously computed signatures, checking the mismatch against the database of exceptions.

15

5

- 13. A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:
 - a) providing a signature computer;
 - b) computing a signature of a file with the signature computer;
 - c) comparing the computed signature to a file signature previously computed by the signature computer; and
 - d) comparing the computed signature to a file signature previously computed by other than the signature computer.
- 14. A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:
 - a) storing a previously computed signature for a file;
 - b) providing a database of exceptions;
 - c) computing a current signature for the file;
 - d) comparing the computed signature to the previously computed signature; and
 - e) if there is a mismatch between the computed and previously computed signatures, checking the mismatch against the database of exceptions.

20